# An Efficient Scheme for Securing Data Warehouses in the Cloud by Reducing Overhead While Enforcing Data Privacy

Veenababu Kannika Sherly

Research Analyst, SMRVD Security Solutions, India.

**Abstract:** In cloud computing schemes, Infrastructure as a Service represents a cloud-computing technology that delivers computing resources, networking, and storage to consumers on-demand, over the internet. It enables end customer or end users to upscale or downsize resources on an as-when needed basis, reducing the need for upscaling, up-front capital expenditures or unnecessary infrastructure. In this paper, we propose an efficient additive encryption scheme based on Shamir's secret sharing for securing data warehouses in the cloud that addresses the shortcomings of existing approaches by reducing overhead while still enforcing good data privacy.

## 1. Introduction

The continued advancement of information technology and data communications strengthens the exchange of highly sensitive medical information. electronic health systems are widely used, and many medical facilities rely on the transmission and receipt of medical information online and on local networks. Over the years, many security systems have been introduced sqto monitor patient privacy and ensure the safety of interchangeable medical data. Cryptography is one of the techniques that often provides security for eHealth systems [1-5].

Nowadays, data outsourcing scenarios tremendously grow with the advent of cloud computing that offers both cost savings and service benefits. One of the most noteworthy cloud outsourcing services is Database-as-a-Service, where individuals and organizations outsource data storage and management to a Cloud Service Provider (CSP) [6-17]. Naturally, such services allow outsourcing a DW and running OLAP queries. Yet, data outsourcing brings out privacy concerns since sensitive data are stored, maintained and processed by an external thirdparty that may not be fully trusted.

A typical solution to preserve data privacy is encrypting data locally be-fore sending them to an external server. Secure database management systems (SDBMSs) such as CryptDB implement cryptographic schemes [18-29]. Paillier's partially homomorphic encryption scheme is notably used in CryptDB to provide high security. However, it induces a

high storage and computation over-head. We propose a new Secure Secret Splitting Scheme (S4) that aims at replacing Paillier's scheme in systems such as CryptDB. S4 is based on the idea of secret sharing and is efficient both in terms of storage and computing, without sacrificing privacy too much.

CryptDB brings together powerful cryptographic tools to handle query processing on encrypted data without decryption. Encryption in CryptDB is like onion layers that store multiple ciphertexts, i.e., encrypted data, within each other. Each onion layer enables certain kind of query processing and a given security level provided by one encryption scheme [30-43]. For instance, order-preserving encryption (OPE) enables range queries and additive hemimorphic encryption enables addition over encrypted data. Yet, CryptDB is not perfectly secured since schemes such as OPE reveal some statistical information about plaintext. MONOMI builds upon CryptDB to allow the execution of analytical work-loads over encrypted data outsourced to the cloud. MONOMI aims at im-proving CryptDB's query processing capability and efficiency based on split client/server execution. A designer also optimizes physical data layout [44-61]. Eventually, using a local trusted hardware at the CSP's, such as TrustedDB and CipherBase, is an alternative approach to query encrypted data. How-ever, trusted hardware is limited in computation ability and memory capacity, and also very expensive.

Fully homomorphic encryption (FHE) allows performing arbitrary arithmetic operations over encrypted data without decryption. FHE provides semantic security, i.e., it is computationally impossible to distinguish two cipher texts encrypted from the same plaintext. However, FHE requires so much computing power that it cannot be used in practice. Partially homomorphic encryption (PHE) is more efficient than FHE. Paillier's the most efficient additive FHE. With Paillier's scheme, multiplying the encryption of two values results in an encryption of the sum of the values, i.e., $Enc_k(x)\ Enc_k(y) = Enc_k(x + y)$, where the multiplication is performed modulo some public-key k. Paillier's scheme is, however, still computation-ally intensive and induces as large ciphertext sizes as 2048 bits. Additionally, modular multiplications become computationally expensive on a large number of records, such as in the fact counter of a DW.

Secret sharing divides a secret piece of data into so-called shares that are stored at n participants'. A subset of k n participants is required to reconstruct the secret. In Shamir's, the rst secret S4's driving idea is based on secret sharing, but instead of sharing secrets to n participants' or CSPs', they are stored at one single CSP's. Thus, we avoid the high storage

overhead of secret sharing. In S4, each secret $v_j$ is divided into n = k splits $v_{1;j}$; :::; $v_{k;j}$. k 1 splits, $v_{1;j}$; :::; $v_{k1;j}$, are stored at the CSP's and $v_{k;j}$ is stored in a trusted machine, e.g., at the user's. In order to reduce storage overhead at the user's, $v_{k;j}$ is set to be the same for all secrets.

## 2. Methodology

First, $x_k$ and $v_k$ are randomly set up from $F_p$, where p is a big prime number, i.e., greater than the greatest possible query answer. For any secret $v_j$, a random polynomial $P_{vj}$ (x) is built that passes through (0; $v_j$) and ($x_k$; $v_k$). To this end, k--2 points ($a_i$; $b_i$); i = 1; :::; k 2 are chosen randomly from $F_p$ such that $a_i$ 6= $x_k$ and $a_i$ 6= 0 8i = 1; :::; k 2. Given k points ($a_1$; $b_1$); ($a_2$; $b_2$); :::; ($a_{k2}$; $b_{k2}$), (0; $v_j$) and ($x_k$; $v_k$), polynomial $P_{vj}$ (x) is built. Storing the k 2 ran-dom points is unnecessary because they are not needed for secret reconstruction.To divide $v_j$ into k 1 splits (since ($x_k$; $v_k$) is already xed), a set of k 1 distinct elements X = f$x_1$; $x_2$; : : : ;$x_{k\ 1}$g is chosen from $F_p$ such that $x_i$ 6= 0and $x_i$ 6= $x_k$ 8i = 1; :::; k 1. Then, splits are $v_{i;j}$ = $P_{vj}$ ($x_i$). K=(X; ($x_k$; $v_k$)) is considered as a private key for S4 and must be kept hidden from the CSP. Tore construct secret $v_j$, its k 1 splits must be retrieved from the CSP. Given points ($x_i$; $v_{i;j}$), i = 1; :::; k 1 and ($x_k$; $v_k$), which is stored at the user's, polynomial $P_{vj}$ (x) can be reconstructed.

Let a relational T consist of one attribute A (additional attributes, if any, can be processed similarly). Suppose T has m records. We denote by $v_j$ the $j^{th}$ value of A. For attribute A in T , k 1 attributes $A_i$, i = 1; :::; k 1 are created in $T^{0}$ at the CSP's, where each attribute $A_i$ stores the $i^{th}$ splits. Without loss of generality, we assume integer data type for other data types can be transformed into integers before splitting. S4 allows summation queries to be computed directly at the CSP's. Consider a query that sums q values of A.

Paillier's PHE is semantically secure, but it is too expensive in terms of cipher-text storage space and query response time. S4 proposes a classical trade-o with a lower level of security, but better storage and response time efficiency. Let us consider a scenario where the CSP is said honest but curious, which is a widely used adversary model for cloud data outsourcing. Such a CSP faithfully complies to any service-level agreement and, in our particular case, stores data, runs queries and provides results without alteration, malicious or otherwise. Yet, the CSP may access data and infer information from queries and results.

Privacy in S4 relies on the fact that a secret value is only retrievable by the user via private key K. As in secret sharing, it is indeed guaranteed that at least k splits and X are necessary to reconstruct a secret, while the CSP has access to only k 1 splits. Both X and the $k^{th}$ split, i.e., K, are stored at the user's. However, the CSP still has access to linear

combinations of splits, which provide some information. Still, the higher k is, the more di cult it is to interpret linear combinations of splits. Thus, k is the prime security parameter in S4. Experiments provide hints for choosing k.

Moreover, if some secrets are known by the CSP, e.g., through public communication of a company to its shareholders. For example, if the CSP knows secrets $v_1$; :::; $v_{k1}$. Also knowing the correspond-ing splits $v_{1;j}$; :::; $v_{k1;j}$ 8j 2 (1; k 1), the CSP can recover the Lagrange basis polynomials $`_i(0)$ 8i 2 (1; k) and recover all secrets. However, the CSP must know at least k 1 secrets to do so. Moreover, we also propose leads to address this problem in next segment.

### 3. Results

We implement S4 in C using compiler gcc 4.8.2. S4's source code is freely available on-line. Experiments related to Paillier's PHE exploit the libpaillier standard C library. All mathematical computations use the GNU Multiple Precision Arithmetic Library (GMP). Eventually, we conduct our experiments on an Intel Core i7 3.10 GHz PC with 16 GB of RAM running Linux Ubuntu 15.05. We compare S4 and Paillier's PHE using simple synthetic datasets, i.e., 32-bit unsigned integers generated uniformly at random from the integer range (103; 104). We scale up the number of records m such that m 2 (103, 104, 105, 106), forming four distinct datasets. In S4, we vary k from 8 to 64, higher values of k inducing too long execution Pm times. Prime p must be greater than the greatest query answer, e.g., p > j=1 vj. In Paillier's PHE, we use a key size of 1024 bits, which induces ciphertexts of 2048 bits. Such key size is the absolute minimum to achieve security.

It is seen that encryption time in S4 is lower than Paillier's when k 16, and then becomes higher when k 16. Secret splitting consists in building a random polynomial by randomly choosing k 2 points. Hence, splitting time increases with k. This actually illustrates the tradeo between S4's security and encryption efficiency with respect to Paillier's PHE. With the selected values of k, decryption is faster with S4 than with Paillier's PHE. This is mainly because Paillier's scheme needs m expensive modular multiplications of large, 2048-bit numbers for decryption, while secret reconstruction in S4 works by polynomial interpolation over k points andevaluating the polynomial in one single point.

With the selected values of k, S4's storage overhead is always much smaller than that of Paillier's PHE since y axis follows a logarithmic scale. Paillier's scheme indeed produces 2048-bit cipher texts. Thus, its storage overhead is m 2048. With S4, each value is split into k

1 values. Thus, S4's storage overhead is m (k 1) times plaintext size. It is seen that, with the selected values of k, query execution time in S4 is lower than that of Paillier's scheme. This is because Paillier's scheme requires m expensive modular multiplications to compute a sum, while S4 computes only (k 1) m simple modular additions.

## 4. Conclusions

We achieved performance gains through a slight degradation of se-curity, especially when an adversary has knowledge of secret values. Although it is definitely satisfactory in some cloud DW and OLAP scenarios, e.g., public aggregate data might not actually yield secrets, i.e., ne-grained data, we will devote future research to strengthen S4 against such threats. More precisely, we plan to introduce noise, as in many cryptographic problems such as approximate-GCD or LWE.

## References

[1] Ahmadi, M.; Moghaddam, F.F.; Jam, A.J.; Gholizadeh, S.; Eslami, M. A 3-level re-encryption model to ensure data protection in cloud computing environments. In Proceedings of the IEEE Conference on System, Process & Control, Kuala Lumpur, Malaysia, 12–14 December 2014.

[2] Surv, N.; Wanve, B.; Kamble, R.; Patil, S.; Katti, J. Framework for client side aes encryption technique in cloud computing. In Proceedings of the IEEE International Advance Computing Conference, Banglore, India, 12–13 June 2015; pp. 525–528.

[3] Singh, S.; Kumar, V. Secured user's authentication and private data storage-access scheme in cloud computing using elliptic curve cryptography. In Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development, New Delhi, India, 11–13 March 2015.

[4] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[5] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[6] Hamid Ali Abed Al-Asadi and et al., "Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network", Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[7] Vinod Varma Vegesna (2015). "Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security," International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[8] Raj, G.; Kesireddi, R.C.; Gupta, S. Enhancement of security mechanism for confidential data using aes-128, 192 and 256 bit encryption in cloud. In Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies, Dehradun, India, 4–5 September 2015.

[9] Latif R., Abbas H., Assar S., Ali Q. Cloud computing risk assessment: a systematic literature review Future Information Technology 2014 Berlin, Germany Springer 285 -295.

[10] Mahmood Z. Data location and security issues in cloud computing Proceedings of the 2nd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT '11) September 2011 IEEE 49-54.

[11] Vinod Varma Vegesna (2021). "The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing," International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[12] Hamid Ali Abed Al-Asadi and et al., "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[13] Hamid Ali Abed Al-Asadi, et al., "Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement", Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[14] Vinod Varma Vegesna (2021). "The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes," International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[15] Stallings, W. Cryptography and Network Security Principles and Practices, 6th ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2005.

[16] Mask Sensitive Data. Available online: https://dataapps.io/redact.html (accessed on 12 January 2017).

[17] Arockiam, L.; Monikandan, S. Efficient cloud storage confidentiality to ensure data security. In Proceedings of the International Conference on Computer Communication and Informatics, Coimbatore, India, 3–5 January 2014; pp. 1–5.

[18] Suthar, K.; Patel, J. EncryScation: A novel framework for cloud iaas, daas security using encryption and obfuscation techniques. In Proceedings of the 2015 5th Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, 26–28 November 2015.

[19] Mar, K.K.; Law, C.Y.; Chin, V. Secure personal cloud storage. In Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), London, UK, 14–16 December 2015.

[20] Vinod Varma Vegesna (2022). “Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications,” International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[21] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[22] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[23] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[24] Vinod Varma Vegesna (2021). “A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments,” International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[25] Sarada, G.; Abitha, N.; Manikandan, G.; Sairam, N. A few new approaches for data

masking. In Proceedings of the 2015 International Conference on Circuit, Power and Computing Technologies, Nagercoil, India, 19–20 March 2015.

[26] Rabin, M.O. Efficient dispersal of information for security, load balancing, and fault tolerance. J. ACM 1989, 36, 335–348.

[27] Li, M. On the Confidentiality of Information Dispersal Algorithms and Their Erasure Codes. arXiv, 2013; arXiv:1206.4123v2.

[28] Jaeger, B. Security as a Service Working Group, Defined Categories of Security as a Service (Preview)—Continuous Monitoring as a Service. Cloud Security Alliance 2016.

[29] Wall, M. Can We Trust Cloud Providers to Keep Our Data Safe? Available online: http://www.bbc.com/news/business-36151754.

[30] White Paper. Securing Sensitive Data within Amazon Web Services Ec2 and Ebs: Challenges and the Solutions to Protecting Data within the AWS Cloud. Copyright 2013 Vormetric. Available online: http://go.thalesesecurity.com/rs/480-LWA-970/images/wp-securing-data-within-AWS.pdf

[31] Zhang, X.; Wang, H. A study of the use of idas in cloud storage. Int. J. Future Comput. Commun. 2013, 2, 67.

[32] Vinod Varma Vegesna (2017). “Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis,” International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[33] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[34] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[35] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[36] Vinod Varma Vegesna (2016). “Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain,” International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[37] Rubenking, N.J. The Best Encryption Software of 2017. Available online: http://www.pcmag.com/article/347066/the-best-encryption-software-of-2016.

[38] Pandey A., Tugnayat R. M., Tiwari A. K. Data Security Framework for Cloud Computing Networks International Journal of Computer Engineering & Technology 2013 4 1 178 -181.

[39] Klein D.A. Data security for digital data storage U.S. Patent Application 14/022,095, 2013.

[40] Biedermann S., Katzenbeisser S. POSTER: event-based isolation of critical data in the cloud Proceedings of the ACM SIGSAC Conference on Computer & Communications Security 2013 ACM 1383-1386.

[41] Delettre C., Boudaoud K., Riveill M. Cloud computing, security and data concealment Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11) July 2011 Kerkyra, Greece 424-431.

[42] Tang Y., Lee P. P. C., Lui J. C. S., Perlman R. Fade: secure overlay cloud storage with file assured deletion Security and Privacy in Communication Networks 2010 New York, NY, USA Springer 380-397.

[43] Vinod Varma Vegesna (2020). “Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications,” Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[44] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[45] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach”, European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[46] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten

Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[47] Vinod Varma Vegesna (2019). “Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes”, Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[48] Sun D., Chang G., Sun L., Wang X. Surveying and analyzing security, privacy and trust issues in cloud computing environments Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS '11) August 2011 chn 2852-2856.

[49] S., Çelik S., Bingöl M. A., Levi A. A new security and privacy framework for RFID in cloud computing Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13) 2013 Bristol, UK.

[50] Behl A. Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation Proceedings of the World Congress on Information and Communication Technologies (WICT '11) December 2011 IEEE 217-222.

[51] Vinod Varma Vegesna (2022). “Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues,” International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[52] Vinod Varma Vegesna (2022). “Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions,” Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[53] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[54] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, “Fuzzy Logic approach to Recognition of Isolated Arabic Characters”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[55] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers," Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[56] Balamurugan, S.; Sathyanarayana, S.; Manikandasaran, S.S. ESSAO: Enhanced security service algorithm using data obfuscation technique to protect data in public cloud storage. Indian J. Sci. Technol. 2016, 9.

[57] Finite Field. Available online: https://en.wikipedia.org/wiki/Finite_field.

[58] Minowa, T.; Takahashi, T. Secure Distributed Storage for Bulk Data; Springer: Berlin/Heidelberg, Germany, 2012; pp. 566–575.

[59] Chen D., Zhao H. Data security and privacy protection issues in cloud computing 1 Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12) March 2012 Hangzhou, China 647-651.

[60] Bowers K. D., Juels A., Oprea A. Proofs of retrievability: theory and implementation Proceedings of the ACM Workshop on Cloud Computing Security (CCSW '09) November 2009 43-53.

[61] Bowers K. D., Juels A., Oprea A. HAIL: a high-availability and integrity layer for cloud storage Proceedings of the 16th ACM conference on Computer and Communications Security November 2009 Chicago, Ill, USA ACM 187-198.